SECRET

See file ADP 3-4 DI for OS attachment to this memo.

OIT 0688-88

29 JUN 1988

MEMORANDUM FOR: Deputy Director for Intelligence

VIA: Deputy Director for Administration

FROM: Edward J. Maloney
Director of Information Technology, DA

SUBJECT: NFIB Coordination on Proposed DCID 1/16 [redacted] 25X1

REFERENCE: Memo for NFIB Principals from Executive Secretary, NFIB, dated 31 May 1988, Subject: Revision of DCID 1/16 (NFIB 5.1/98), with attachments

1. The reference requests coordination of proposed DCID 1/16, Security Policy for Uniform Protection of Intelligence Processed in Automated Information Systems and Networks. The proposed DCID is a very complex document with major policy and resource implications for the Agency. One potential problem area is a change in the policy governing the protection of Sensitive Compartmented Information (SCI) in Automated Information Systems (AISs). A second major topic of concern is the unevaluated, but inevitably large, resource implications of the required AIS security enhancements and accreditation procedures. These two concerns alone warrant further study by the Agency prior to formal concurrence. [redacted] 25X1

2. The proposed policy will allow users with only Secret clearances to access multilevel systems processing SCI provided either the DCI, DIRNSA, or D/DIA "personally" authorizes such. This seems to be a significant change from the present, more conservative policy which restricts access to users possessing a Top Secret clearance based on DCID 1/14 standards. Since "multilevel" system security technology and accreditation procedures are yet to be proven and risk assessment is not yet standardized, we recommend this policy change be approached with extreme caution. [redacted] 25X1

3. We have not been able to fully evaluate the total resource needs to implement the new DCID, but they appear to be very significant. In addition to our knowledge, no Agency or component has "walked" through the procedures set forth in the accompanying Security Manual to verify that the requirements and procedures are both necessary and sufficient. Further study is needed before the Community becomes locked into a policy for which implementation may turn out to be impractical either for resource or technical reasons. [redacted] 25X1

[redacted] 25X1

SECRET

SUBJECT: NFIB Coordination on Proposed DCID 1/16 [redacted] 25X1

4. Additional OIT comments are provided in Attachment A. Please note that a complete evaluation and formal Directorate coordination were not possible given the extremely tight deadline for review of a very complex document. Office of Security comments will be forwarded separately. Office of Communications comments are, however, reflected herein. The OIT referent for DCID 1/16 is [redacted], Chief, Technical Security Staff. 25X1
[redacted] may be reached on [redacted] 25X1

Edward J. Maloney

Attachment:
As stated

SUBJECT: NFIB Coordination on Proposed DCID 1/16 [redacted] 25X1

TSS/OIT [redacted] (29 June 88) 25X1

Distribution:
Orig - Addressee (w/att)
1 - DDA (w/att)
2 - DDA Registry (w/att)
1 - D/OC (w/att)
2 - D/OIT (w/att)
1 - MSD/MG/OIT (w/att)
3 - ISC (w/att)

ATTACHMENT A
to DCID 1/16 Comments

1. The proposed DCID 1/16 is a confusing document which mixes policy, goals, operations, and implementation concepts. Any revision should remain a clear statement of policy. Computer security goals should be stated along with other NFIB goals in appropriate DCI guidance documents; operations and implementation concepts should be placed in supporting documents as in the current DCID 1/16.

2. Much of the confusion results from seeming inconsistences between the basic policy document and the accompanying Security Manual. For example:

(1) Paragraph 1a of the basic policy document states that the Security Manual provides specific guidance for policy implementation. Paragraph 1 of the introduction to the Security Manual states the provisions of the manual has the same force as the basic directive. If this is truly intended, this provision ought to be clearly stated in the basic document.

(2) Confusion is bound to arise from the provision of Paragraph 3a of the basic document. This paragraph states that the Accrediting Authority "formally assumes security responsibility" for the system he/she accredits. Such Accrediting Authority may or may not have operational control and responsibility for said system. Realistically, could the DCI, DIRNSA, and D/DIA personally assume such responsibility for a multilevel system owned and operated by the White House, DOS, or DOE?

(3) Finally, the "wordiness" of the documents adds to the difficulty of interpreting and understanding exactly what the policy is. It may be wise to rework, if only for that purpose.